DEALING WITH CYBERBULLIES

Though DIR's Cyber Security Tips often relate to workplace cyber security, cyberbullying, or harassment through electronic messaging, can affect adults at work or at home. However, it is more common for youth to be exposed to this dangerous behavior. Cyberbullying can occur via cell phone text messaging, email, instant messaging, or even within online gaming and social networking sites. The threats, rumors, abuse, and lies often used in cyberbullying are not only difficult to escape, but they can also have long lasting, detrimental effects on children.

In an effort to educate our citizens and protect our youth from this growing trend, DIR offers these tips on how to identify and protect yourself and your children from cyberbullies. In addition, useful resources and guides are also included at the end of this newsletter. Please feel free to share this with your family and friends.

Bullies are now taking advantage of technology to intimidate and harass their victims. Dealing with cyberbullying can be difficult, but there are steps you can take.

WHAT IS CYBERBULLYING?

Cyberbullying refers to the new and growing practice of using technology to harass, or bully, someone else. Bullies used to be restricted to methods such as physical intimidation, postal mail, or the telephone. Now, developments in electronic media offer forums such as email, instant messaging, web pages, and digital photos to add to the arsenal. Computers, cell phones, and PDAs are new tools that can be applied to an old practice.

Forms of cyberbullying can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking. It can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools.

WHY HAS CYBERBULLYING BECOME SUCH A PROBLEM?

The relative anonymity of the Internet is appealing for bullies because it enhances the intimidation and makes tracing the activity more difficult. Some bullies also find it easier to be more vicious because there is no personal contact. Unfortunately, the Internet and email can also increase the visibility of the activity. Information or pictures posted online or forwarded in mass emails can reach a larger audience faster than more traditional methods, causing more damage to the victims. And because of the amount of personal information available online, bullies may be able to choose their victims arbitrarily.

Cyberbullying may also indicate a tendency toward more serious behavior. While bullying has always been an unfortunate reality, most bullies grow out of it. Cyberbullying has not existed long enough to have solid research, but there is evidence that it may be an early warning for more violent behavior.

HOW CAN PROTECT MYSELF?

- **Be careful where you post personal information** – By limiting the number of people who have access to your contact information or details about your interests, habits, or employment, you can reduce your exposure to bullies that you do not know. This may limit your risk of becoming a victim and may make it easier to identify the bully if you are victimized.

- **Avoiding escalating the situation** – Responding with hostility is likely to provoke a bully and escalate the situation. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. Other options include subtle actions. For example, if you are receiving unwanted email messages, consider changing your email address. If the bully does not have access to the new address, the problem may stop. If you continue to receive messages at your new account, you may have a stronger case for legal action.

- **Document the activity** – Keep a record of all online activity (emails, web pages, instant messages, etc.) including relevant dates and times. In addition to archiving an electronic version, consider printing a copy.

- **Report cyberbullying to the appropriate authorities** – If you are being harassed or threatened, report the activity to the local authorities. Law enforcement agencies have different policies, but your local police department or FBI branch are good starting points. Unfortunately, there is a distinction between free speech and punishable offenses, but the legal implications should be decided by the law enforcement officials and the prosecutors. Depending on the activity, it may also be appropriate to report it to school officials who may have separate policies for dealing with activity that involves students.

Protect your children by teaching them good online habits (see **Keeping Children Safe Online** – **www.us-cert.gov/cas/tips/ST05-002.html**). Keep lines of communication open with your children so that they feel comfortable telling you if they are being victimized online. Reduce their risk of becoming cyberbullies by setting guidelines for and monitoring their use of the Internet and other electronic media (cell phones, PDAs, etc.).

ADDITIONAL RESOURCES

The following sites offer additional guidance for protecting you and your children from cyberbullies:

- The Internet Keep Safe Coalition (**www.ikeepsafe.org**) group teaches basic rules of Internet safety to children and parents, reaching them online at IKeepSafe.org and in school. They seek to teach children the *three keeps*:

    - **I Keep Safe** all my personal information.

    - **I Keep Away** from online strangers.

    - **I Keep Telling** my parents or a trusted adult what I see on the Internet.

- *McGruff.org* (**www.mcgruff.org/advice/cyberbullies.php**) has a short tip list for kids and in addition has created a short game called *Shrink the Cyberbully* to help kids learn strategies to help stop cyber bullying.

- *Power In You* (**www.powerinyou.org/?id=MzI2**) is an effort to help children and teens with many challenges, including bullying.

- Microsoft created *10 tips for dealing with game cyberbullies and griefers* (**www.microsoft.com/athome/security/children/griefers.mspx**).

- *USA Today* and *StaySafeOnline* published *High-tech bullying may be on the rise* (**www.usatoday.com/educate/cybersecurity/20060927-cyber4-bullying.pdf**), an educational article that includes discussion points, a learning activity for family and friends, tips, and an activity sheet to help children prepare for and react to cyberbullying.

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by:	Powered by:	Distributed by:
www.msisac.org	**www.us-cert.gov**	**www.dir.state.tx.us/securetexas**

Copyright Carnegie Mellon University | Produced by US-CERT